⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2－266465

⑤1Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)10月31日
G 06 F 15/30	340	6798－5B	
G 09 C 1/00		7343－5B	

審査請求　未請求　請求項の数 3　（全9頁）

⑤4発明の名称　認証方式

⑳特　願　平1－87272
㉒出　願　平1(1989)4月5日

⑦2発明者　岡本　龍明　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
⑦2発明者　太田　和夫　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
⑦1出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号
⑦4代理人　弁理士　草野　卓

明　細　書

1．発明の名称

認証方式

2．特許請求の範囲

（1）　通信相手の身元を確認する利用者の認証方式において、

証明者Aと被検証者Bと検証者Cから構成されたシステムで、

証明者Aは初期応答文発生器と証明器を備え、被検証者Bは乱数発生器，初期応答文攪乱器，問い合わせ文攪乱器と乱数成文除去器を備え、検証者Cは検査器を備え、

証明者Aは、初期応答文発生器を用いて生成した初期応答文x'を個人識別情報IDと共に被検証者Bに送信し、

被検証者Bは、証明者Aから受信した初期応答文x'と乱数発生器を用いて生成した乱数成分を初期応答文攪乱器に入力して初期応答文x"を作成して受信したIDと共に検証者Cに送信し、

検証者Cは、被検証者Bに問い合わせ文βを送信し、

被検証者Bは、Cから受信した問い合わせ文βと先に生成した乱数成分を問い合わせ文攪乱器に入力して問い合わせ文β'を作成して証明者Aに送信し、

証明者Aは、初期応答文x'と問い合わせ文β'に対応した応答文zを、IDに対した関係式 $s_j^2 \bmod N = f(ID,j)$ をみたす秘密情報s_jを用いて動作する証明器を用いて生成して被検証者Bに送り返し（ここで、整数Nと関数fは公開情報）、

被検証者Bは応答文zとIDを乱数成分除去器に入力して乱数成分の影響を取り除いて応答文z'を求め、その値を検証者Cに送信し、

検証者Cは応答文z'とIDを検査器に入力してz'が先に受信した初期応答文x"と先に送信した問い合わせ文βに対する正しい応答になっていることを検査して、

被検証者Bが乱数成分を秘密にすることで、被検証者Bと証明者A間で通信されるx'，β'，

zと、検証者Cと被検証者B間で通信されるx''，β，z'の対応関係を秘密にできることを特徴とする利用者の認証方式。

（2） 請求項（1）に記載の手順を繰り返して、安全性を向上する利用者の認証方式。

（3） 通信文の正当性を確認するメッセージの認証方式において、

証明者Aと被検証者Bと検証者Cから構成されたシステムで、

証明者Aは初期応答文発生器と証明器を備え、被検証者Bは乱数発生器，初期応答文撹乱器，問い合わせ文発生器と乱数成文除去器を備え、検証者Cは検査器を備え、

証明者Aは、初期応答文発生器を用いて生成した初期応答文x'を個人識別情報IDと共に被検証者Bに送信し、

被検証者Bは、証明者Aから受信した初期応答文x'とIDと乱数発生器を用いて生成した乱数成分とを初期応答文撹乱器に入力して初期応答文x''を作成し、その初期応答文x''と署名対象のメッセージmを問い合わせ文発生器に入力して問い合わせ文βとβ'を作成してβ'を証明者Aに送信し、

証明者Aは、先に送信した初期応答文x'と受信した問い合わせ文β'に対応した応答文zを、IDに対した関係式$s_j^2 \bmod N = f(ID, j)$をみたす秘密情報s_jを用いて動作する証明器を用いて生成して被検証者Bに送り返し（ここで、整数Nと関数fは公開情報）、

被検証者Bは応答文zとIDと先に生成した乱数成分と問い合わせ文βを乱数成分除去器に入力して乱数成分の影響を取り除いてメッセージmに対応した値z'を求め、z'をm，ID，βと共に検証者Cに送信し、

検証者Cはz'とメッセージmと問い合わせ文βとIDを検査器に入力してβとz'がmに対する正しい署名になっていることを検査して、

被検証者Bが乱数成分を秘密にすることで、被検証者Bと証明者A間で通信されるx'，β'，zと、検証者Cと被検証者B間で通信されるm，β，z'の対応関係を秘密にできることを特徴とするメッセージの認証方式。

3．発明の詳細な説明

「産業上の利用分野」

この発明は、電気通信システムで電子資金移動等を行う場合に、消費者のプライバシィを保護できる通信プロトコルを実現できる認証方式である。

「従来の技術」

電気通信システムを用いた電子資金移動やICカードを用いた決済が普及している。また、現金の代替手段としての汎用プリペイドカードの利用法や、電子財布の使用法が研究されている。このとき、資金の流れが特定の組織に管理されると、消費者の消費動向等の個人情報がその組織に蓄積され、プライバシィ保護の観点から問題となる。

この問題の解決策として、暗号技術を用いて、資金移動の追跡を不可能とする安全な資金移動方式がある。例えば、David Chaum："Security without Identification : Transaction systems to make Big Brother Obsolute", Communication of the ACM, October 1985, Vol. 28 No. 10

Chaumの方式の概要は以下の通りである。

消費者（被検証者：B）が金額等の取引内容を含んだ文書mを乱数で撹乱して通信文zを作成して、zを銀行（証明者：A）に送信する。銀行Aは、消費者Bの正当性を認証した後にその消費者の口座から金額を引き落とし、金額に対応した署名をzに施して、署名付き通信文z'を消費者Bに送り返す。消費者Bは、z'から乱数の影響を取り除いて、mに署名を施した値としてm'を求め、これを現金にかわる手段として商店（検証者：C）へ支払う。検証者Cは、m'が銀行Aによって署名されていることを確認して、m'がある金額の価値があると判断する。Cは後日m'を銀行Aに提出することによって、対応する金額を受け取る。すなわち、m'は金券としての機能を備えている。

ここで、zはmに乱数が付加されているので、銀行および第三者はzからmを推定できないし、また、銀行と商店が結託してもm'とzの対応を

知ることができない。従って誰がm'を発行したかを知ることができない。これより、Chaum の方法では金券m'の発行元（消費者）を推定できない（すなわち、追跡不可能）ので、消費者の消費動向等のプライバシィを守ることができる。

しかし、この方式は処理量の大きいＲＳＡ暗号をベースにしているので、zからz'を求めるための処理量の大きいことが問題となる（この例では銀行Ａの処理量が大きくなる）。具体的には、ＲＳＡ暗号では、２００桁同志の整数の乗法（ただし剰余計算を含む）が平均７６８回必要である。

ところで、高速な認証方式として FiatとShamirの方式がある（ Fiat,A. and Shamir,A: "How to prove yourself : practical solutions to identification and signature problems", Proceedings of Crypto 86, Santa Barbara, August 1986, pp. 18-1-18-7)。

Fiat－Shamir法では、処理量は、平均してｔ（ｋ＋２）／２回の乗算（ただし法Ｎにおける剰余計算を含む）で済む（ｋとｔの意味は後述）、特に、ｋ＝５，ｔ＝４に選ぶことが推奨されているので、この場合には、Fiat-Shamir 法の乗算回数は１４回となり、ＲＳＡ暗号による署名法に比較して処理量を大幅に削減できる。具体的には、１４／７６８＝0.０２なのでＲＳＡ暗号に比べて約２％の処理量で実現できる。

Fiat-Shamir 法の概要は、以下の通りである。

信頼できるセンタが、個人識別情報としてＩＤを用いる利用者に対して、次の手順でｋ個の秘密情報s_j（$1 \leq j \leq k$）を生成する（ｋは安全性を定めるパラメータであり１以上の値）。ここでＮは公開情報であり、秘密の素数ＰとＱを用いてＮ＝Ｐ×Ｑと表せる。またｆは一方向性関数であり、公開されている。

step1 : 一方向性関数ｆを用いて

$$x_j = f(ID, j) \quad (1 \leq j \leq k)$$

を計算する。

step2 : 各x_jに対してＮの素因数ＰとＱを用いて

$$s_j = \sqrt{x_j} \pmod N$$

を計算する。すなわち、$s_j^2 = x_j \pmod N$となる。

注)Fiat-Shamir法では、実際には$s_j = \sqrt{1/x_j}$としているが、上記のようにs_jを定めても同様の議論が成り立つ。

step3 : 利用者に対してｋ個のs_jを秘密に発行し、一方向性関数ｆと合成数Ｎを公開する。

（ｍｏｄ　Ｎ）における平方根の計算は、Ｎの素因数（ＰとＱ）が分かっているときのみ実行できる。その方法は、例えば Rabin,M.O.: "Digita- lized Signatures and Public-Key Functions as Intractable as Factorization ", Tech. Rep. MIT/LCS/TR-212 MIT Lab. Comput. Sci. 1979 に示されている。平方根の計算装置の具体的な構成例は、公開鍵暗号システム（特願昭61-169350)に示されている。

利用者の認証方式は以下の通りである。

証明者Ａは、検証者Ｃに対して、Ａが本物であることを、次の手順で証明する。

step1 : ＡがＩＤをＣに送る。

step2 : Ｃが$x_j = f(ID, j)$ $(1 \leq j \leq k)$を計算する。

次に、ｉ＝１，…，ｔについて３～６のステップを繰り返す（ｔは安全性を定めるパラメータであり、１以上の値）。

step3 : 乱数r_iを生成して、

$$x'_i = r_i^2 \pmod N$$

を計算して、Ｃに送る。

step4 : Ｃが、０，１のビット列（e_{i1}, …, e_{ik}）を生成して、Ａに送る。

step5 : Ａが署名文z_iを

$$z_i = r_i \prod_{e_{ij}=1} s_j \pmod N$$

で生成して、Ｃに送る。

step6 : Ｃは、

$$x'_i = z_i^2 / \prod_{e_{ij}=1} x_j \pmod N$$

が成り立つことを検査する。

z_i の作り方より $z_i^2 / \prod_{e_{ij}=1} x_j = r_i^2 \prod_{e_{ij}=1}$

$(s_j^2 \times x_j^{-1}) = r_i^2 = x'_i \pmod N$

であるから、t回の検査にすべて合格した場合、検証者CはAが本物であると認める。

このとき、検証者Cが、偽の証明者を本物のAと認めてしまう誤りの生じる確率は $1/2^{kt}$ である。ここで、kは証明者が秘密に管理する s_j の個数であり、tは通信文の通信回数を定めている。

以上では、利用者の認証方式について説明したが、メッセージの認証方式は上記の手順を次の様に変更して実現できる。

メッセージmと $(x'_1, \cdots, x'_t)$ に一方向性関数fを施して得た $f(m, x'_1, \cdots, x'_t)$ の先頭のk×tビットを上記手順のビット列 (e_{ij}) とみなして、署名文として、(ID, m, (e_{ij}), $z_1, \cdots, z_t$) を署名つき通信文として検証者に送信する。

このようにFiat-Shamir 法は高速な認証方式であるが、現在までのところFiat-Shamir 法を用いた追跡不可能な認証方式は提案されていない。

「発明が解決しようとする課題」

この発明の目的は、システム設計者が処理速度を考慮して安全性のパラメータを選択できるようにして、従来方式よりも高速な追跡不可能な認証方式を提供することにある。

「課題を解決するための手段」

この発明では、処理量を削減するために、問い合わせ文と応答文を用いるFiat-Shamir 法をベースにして、高速な認証処理を実現する。また、第三者にA－B間とB－C間で通信されるデータの対応関係を隠して、追跡不可能とするために、Bが問い合わせ文の対応関係と応答文の対応関係を乱数によって与え、その乱数を秘密にする。これによって、この発明では、追跡不可能な認証処理を、従来より少ない処理量で実現する。

「実施例」

第1図は、この発明の原理図である。第1図は証明者A（100）と被検証者B（200）と検証者C（300）が通信回線を介して接続しており、利用者の認証方式（図（a））とメッセージの認証方式（図（b））を実現するための交信例を表している。以下では、先ず、AがBの身元を確認したことをCに対して証明する利用者の認証方式を示し、その後に、BがAの力を借りてメッセージmに署名するメッセージの認証方式について説明する。

第1図の（a）では、A－B間とB－C間でそれぞれFiat-Shamir 法の利用者認証法を採用し、2つのFiat-Shamir 法を対応づける情報をBにおいて秘密にすることで、追跡不可能な利用者の認証処理を実現する。

Fiat-Shamir 法の場合と同様に、信頼できるセンタが、合成数Nと一方向性関数fを公開し、さらに証明者Aの識別情報IDに対応する秘密情報 s_j を計算して、s_j をAに配送する。ここで、s_j は、$s_j^2 \bmod N = x_j = f(ID, j)$ をみたすことに注意。

A（100）の概略を第2図に、B（200）の概略を第3図に、C（300）の概略を第4図にそれぞれ示す。

証明者Aは、被検証者Bの正当性を、検証者Cに対して、次の手順で証明する。

step1 ： AがIDをBとCに送る。

step2 ： BとCは、それぞれ一方向性関数計算器205, 305を用いて $x_j = f(ID, j)$ を計算する。

次に、3～6のステップをt回繰り返す。t＝1のときが特許請求範囲の請求項（1）に対応し、t＞1のときが請求項（2）に対応する。

step3 ： Aは初期応答文発生器110を用いて初期応答文x'を発生してBに送る。

例えば初期応答文発生器110を乱数発生器111と剰余付き乗算器112で構成して、乱数発生器111を用いて乱数rを発生し、剰余付き乗算器112を用いて

$x' = r^z \pmod N$

でx'を計算する。

剰余付き乗算の効率のよい計算方法は、例えば

池野，小山“現代暗号理論”電子通信学会，pp. 16－17，（１９８６），に示されている。

step4 ：Ｂはｘ’を受信すると、乱数発生器２１０と初期応答文撹乱器２１５を用いて，乱数発生器２１０で発生したｋ個の０，１のビット｛ｅ$_j$｝と乱数ｕをｘ’と先に生成したｘと共に初期応答文撹乱器２１５に入力し、撹乱された初期応答文ｘ”を計算してＣに送る。

例えば初期応答文撹乱器２１５を剰余付き乗算器として構成し、受信した初期応答文ｘ’とｘ$_j$と｛ｅ$_j$｝とｕから

$$x'' = x' \times u^{z} \times \prod_{e_j=1} x_j \quad (\mathrm{mod}\ N)$$

でｘ”を計算する。

step5 ：Ｃはｘ”を受信すると、ｘ”を秘密情報格納器３１０に格納した後に、乱数発生器３２０を用いて、ｋ個の０，１のビット｛β_j｝を生成してβ＝（β_1，…，β_k）を問い合わせ文としてＢに送る。

step6 ：Ｂはβを受信すると、βと先に生成した｛ｅ$_j$｝を問い合わせ文撹乱器２２０に入力して、撹乱された問い合わせ文β'＝（β'_1，…，β'_k）を計算してＡに送る。

例えば問い合わせ文撹乱器２２０を排他的論理和計算器として構成して、

$$\beta'_j = \beta_j \oplus e_j$$

を計算する。

step7 ：Ａはβ'を受信すると、先に生成した乱数ｒと受信した問い合わせ文β'を証明器１２０に入力して、応答文ｚを計算してＢに送る。

例えば証明器１２０を、秘密情報格納器 121 と剰余付き乗算器１２２で構成し、秘密情報格納器１２１から秘密情報｛ｓ$_j$｝を読み出して、初期応答文発生器１１０から引き継いだｒと受信したβ'を剰余付き乗算器１２２に入力して

$$z = r \times \prod_{\beta'_j=1} s_j \quad (\mathrm{mod}\ N)$$

でｚを計算する。

step8 ：Ｂはｚを受信すると、ｚと先に生成した｛ｘ$_j$｝と｛ｅ$_j$｝とｕを乱数成分除去器２３０に入力して、応答文ｚ’を計算してＣに送る。

例えば乱数成分除去器２３０を、条件判定器２３１と剰余付き乗算器２３２で構成し、

$$z' = u \times z \times \prod_{c_j=1} x_j \quad (\mathrm{mod}\ N)$$

ただし、ｃ$_j$＝β_j and ｅ$_j$

を計算する。

step9 ：Ｃはｚ’を受信すると、検査器３３０を用いてｚ’の正当性を検査する。

例えば検査器３３０を、剰余付き乗算器 331 と比較器332 で構成し、秘密情報格納器310 から引き継いだｘ”と一方向性関数計算器305 から引き継いだｘ$_j$と乱数発生器３２０から引き継いだβに対して

$$x'' = z'^{z} / \prod_{\beta_j=1} x_j \quad (\mathrm{mod}\ N)$$

が成立するかを検査する。

ここではｔ回の問い合わせ－応答のやりとりを順次行う例を示したが、問い合わせ－応答のやりとりを同時に行ってもよい。

次に、第１図の（ｂ）を用いて、ＢがＡの力を借りてメッセージｍに署名するメッセージの認証方式について説明する。

Ａ－Ｂ間では Fiat-Shamir法の利用者認証法を、Ｂ－Ｃ間では Fiat-Shamir法のメッセージ認証法を採用する。２つの認証法を対応づける情報をＢにおいて秘密にすることで、追跡不可能なメッセージの認証処理を実現する。

Fiat-Shamir法と同様に、信頼できるセンタが、合成数Ｎと一方向性関数ｆを公開し、さらに、証明者Ａの識別情報ＩＤに対応する秘密情報｛ｓ$_j$｝を計算して、｛ｓ$_j$｝をＡに配送する。

Ａ（１００）の概略を第２図に、Ｂ（２００）の概略を第５図に、Ｃ（３００）の概略を第６図にそれぞれ示す。

Ｂは、Ａの力を借りて、次の手順で文書ｍに署

名する。

step1 : AがIDをBとCに送る。

step2 : BとCは、それぞれ一方向性関数計算器205,305 を用いて$x_j = f(ID, j)$を計算する。

step3 : Aは初期応答文発生器110を用いてt個の初期応答文x'_i ($i = 1, 2, \cdots, t$)からなるx' を計算してBに送る。

例えば初期応答文発生器110を、乱数発生器111と剰余付き乗算器112で構成し、乱数発生器111を用いてt個のr_iを発生し、剰余付き乗算器112を用いて

$$x'_i = r_i^2 \pmod N \quad (i = 1, 2, \cdots, t)$$

で、t個のx'_iを計算する。

step4 : Bはx' を受信すると、乱数発生器210を用いてt組のkビット$\{e_{ij}\}$と乱数u_iのペアを発生し、その値を受信したt個のx'_iと先に生成した$\{x_j\}$と共に初期応答文撹乱器215に入力し、t個の撹乱された初期応答文x''_iを計算して$x'' = (x''_1, \cdots, x''_t)$を問い合わせ文発生器250に引き継ぐ。

例えば初期応答文撹乱器215を剰余付き乗算器で構成し、乱数発生器210が生成したt組の$\{e_{ij}\}$とu_i, 受信したt個の初期応答文x'_iとx_jを初期応答文撹乱器215に入力して

$$x''_i = x'_i \times u_i^2 \times \prod_{e_{ij}=1} x_j \pmod N \quad (i = 1, 2, \cdots, t)$$

でt個のx''_iを計算する。

step5 : Bは、メッセージmとt個のx''_iを問い合わせ文発生器250に入力して、問い合わせ文βとβ'を作成してβ'をAに送信し、βを乱数成分除去器260に引き継ぐ。

例えば、問い合わせ文発生器250を一方向性関数計算器251と排他的論理和計算器252で構成して、

$$\{\beta_{ij}\} = f(m, x''_1, \cdots, x''_t)$$

$$\beta'_{ij} = \beta_{ij} \oplus e_{ij} \quad (i = 1, 2, \cdots, t,\ j = 1, 2, \cdots, k)$$

で、$\beta = \{\beta_{ij}\}$と$\beta' = \{\beta'_{ij}\}$を求める。

step6 : Aはβ'を受信すると、証明器120を用いて、先に発生した乱数r_iと受信した問い合わせ文β'から、応答文zを計算してBに送る。

例えば証明器120を、秘密情報格納器121と剰余付き乗算器122で構成し、秘密情報格納器121から秘密情報$\{s_j\}$を読み出し、初期応答文発生器110から引き継いだ$\{r_i\}$と受信したβ'を剰余付き乗算器122に入力して

$$z_i = r_i \times \prod_{\beta'_{ij}=1} s_j \pmod N \quad (i = 1, 2, \cdots, t)$$

で計算したz_iを用いて、$z = (z_1, \cdots, z_t)$を求める。

step7 : Bはzを受信すると、zと先に生成した$\{x_j\}$とt組の($\{e_{ij}\}$, u_i)を乱数成分除去器260に入力して、応答文z' を計算して、β, mと共にCに送る。

例えば乱数成分除去器260を、条件判定器261と剰余付き乗算器262で構成し、

$$z'_i = u_i \times z_i \times \prod_{c_{ij}=1} x_j \pmod N \quad (i = 1, 2, \cdots, t)$$

ただし、$c_{ij} = \beta_{ij}$ and e_{ij}

で計算したz'_iを用いて、$z' = (z'_1, \cdots, z'_t)$を求める。

step8 : Cはm, β, z' を受信すると、検査器340を用いてm, β, z' の正当性を検査する。

例えば検査器340を、剰余付き乗算器341と一方向性関数計算器342と比較器343で構成し、

$$x''_i = z'^2_i \,/ \prod_{\beta_{ij}=1} x_j \pmod N$$

で$x'' = (x''_1, \cdots, x''_t)$を求めて、

$\{\beta_{ij}\} = f(m, x^*)$

が成立するかを検査する。

以上では、Fiat-Shamir法をベースにした追跡不可能な認証方式について説明した。Fiat-Shamir法は、Nの素因数分解が困難な場合に(mod N)での平方根の計算が困難なことに基づいている。離散対数問題等の困難性を利用した認証法をベースにしても、同様の議論が成り立つ。離散対数問題等に基づく認証法については、例えば M.Tompa & H.Woll,"Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information," FOCS, pp472-482(1987)や岡本,太田,"零知識証明問題の不正使用法とその対策及び応用について"(1988年暗号と情報セキュリティシンポジウムワークショップ)に示されている。

「発明の効果」

この発明では、Fiat-Shamir 法をベースにしたので、高速な認証処理を実現できる。

また、Bが問い合わせ文の対応関係と応答文の対応関係を秘密の乱数で与えておりその値を秘密にすると、A－B間とB－C間で通信されるデータの対応関係を隠すことができる。すなわち、利用者の認証処理においては、AがBの身元を保障していることを、Bの身元を明かさずに、Cに証明できる。メッセージの認証処理においては、Bはメッセージmの内容を知られることなしにAに署名させることができる。その結果として、AとCが結託しても、Bの身元は明らかとならず、Bがmを送信したことも検出できない。すなわち、追跡不可能な認証処理を実現できる。以上より、この発明では、従来方式より高速に追跡不可能な認証処理を実現できる。

証明者Aと検証者Cが結託しても、被認証者が誰であるかを判断したり、メッセージmの送信者が誰であるかを判断したりできないことは、この発明の方式が計算量理論の理論的な研究成果である零知識対話型証明システム性や非転移性をみたすことによって保障できる。

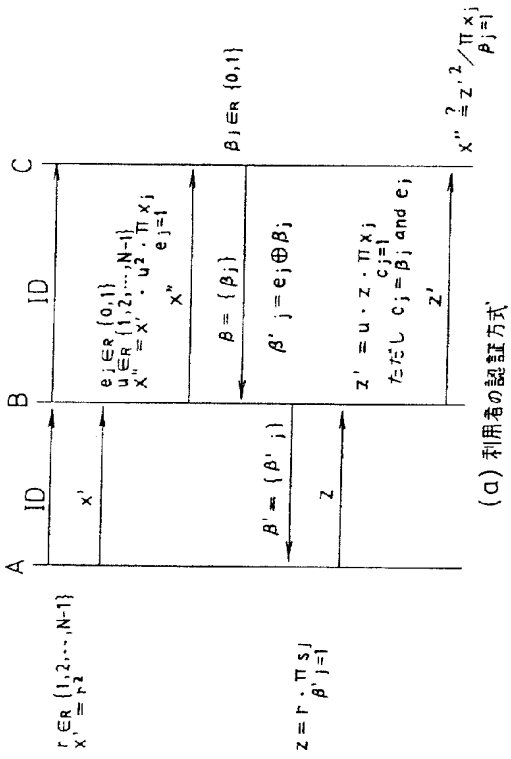
零知識対話型証明システム性および非転移性については、例えば Feige,U.,Fiat,A. and Shamir, A. "Zero Knowledge Proofs of Identity" Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, pp.210-217.を参照。

4．図面の簡単な説明

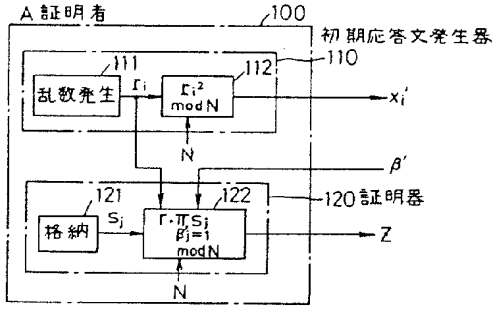
第1図はこの発明の実施例の交信例を示す図、第2図は証明者Aのブロック図、第3図は利用者の認証方式における被検証者Bのブロック図、第4図は利用者の認証方式における検証者Cのブロック図、第5図はメッセージの認証方式における被検証者Bのブロック図、第6図はメッセージの認証方式における検証者Cのブロック図である。

特許出願人　日本電信電話株式会社
代理人　草野　卓

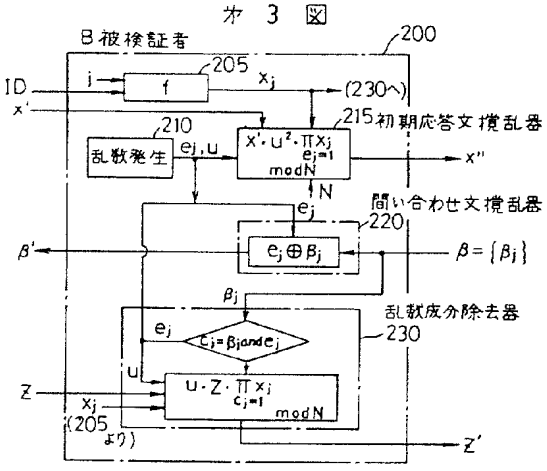
第1図



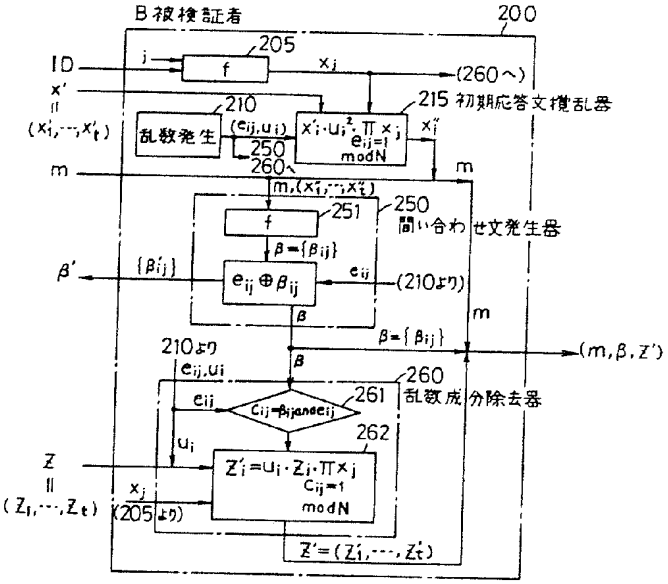
第2図



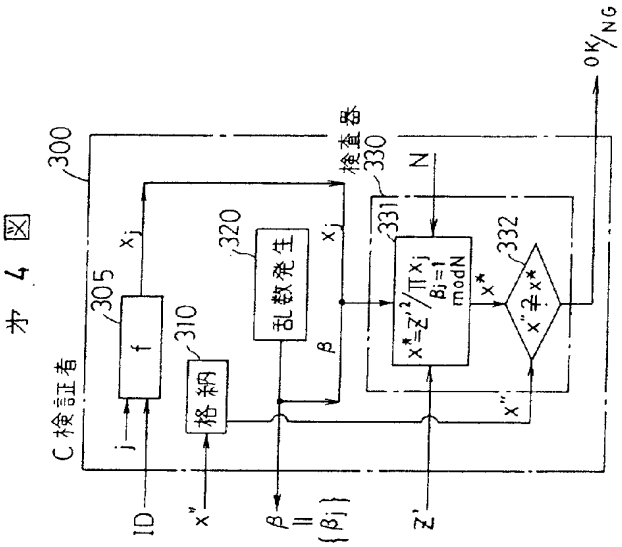
第3図



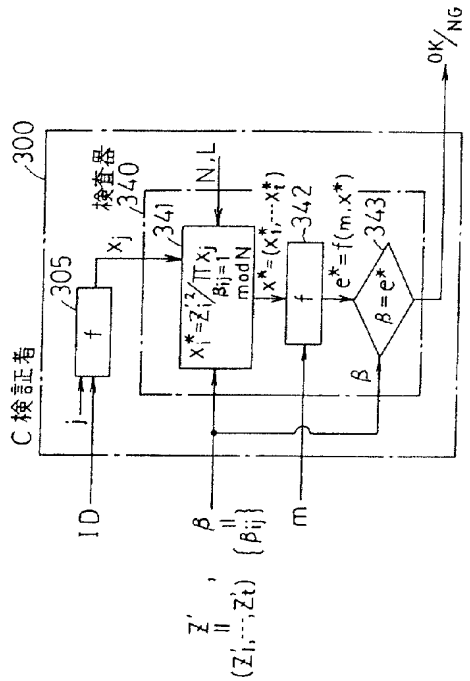
第5図



第4図


300
C検証者
305
f
j
ID
310
格納
x''
320
乱数発生
β
{βj}
検査器
330
331
x*=z'^2/Πxj^βj=1 modN
N
z'
x''
332
x''≠x*
OK/NG

第6図


300
C検証者
305
f
j
ID
検査器
340
341
x1*=z'1^2/Πxj^βij=1 modN
N,L
x*=(x1*,…xt*)
342
f
e*=f(m,x*)
343
β=e*
OK/NG
β
{βij}
z'
(z'1,…,z't)
m